Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) An integrated circuit for the authentication of a consumable storage device by an apparatus, the integrated circuit comprising a memory space which contains encrypted data defined by a message authentication code (MAC) applied to data relating to a consumable stored by the device, the MAC being a construction of an asymmetric cryptographic function whereby a public key K_T of the apparatus is used to decrypt an encrypted random number appended to the data, the random number being encrypted ~~as generated~~ by the public key K_T of another integrated circuit of the apparatus ~~and~~, and a secret key K_A of the apparatus is used to decrypt encrypted data stored in the memory space.

2. (Original) An integrated circuit as claimed in claim 1, in which the cryptographic function is a hash function such that the MAC is an algorithm known as HMAC.

3. (Original) An integrated circuit as claimed in claim 2 in which the hash function is one of an MD5 function and a SHA-1 function.

4. (Original) An integrated circuit as claimed in claim 2, in which the hash function is an SHA-1 function.

5. (Original) An integrated circuit as claimed in claim 4, which is configured to define a number of temporary registers and rotating counters and to calculate an output word on an iterative basis by calculating and allocating words to respective registers during processing of the SHA-1 function.

6. (Cancelled)

7. (Currently Amended) A method of encrypting data relating to a consumable of a consumable storage device for an apparatus and stored by an integrated circuit, the method including the steps of:

applying a message authentication code (MAC) to the data using two keys shared by the apparatus to decrypt the data, the MAC being a construction of an asymmetric cryptographic function whereby one of the keys is a public key used to decrypt an encrypted random number appended to the data, the random number being encrypted ~~as generated~~ by the public key of another integrated circuit of the apparatus ~~and~~, and the other key is a secret key used to decrypt encrypted data stored in the first-mentioned integrated circuit.